Hortonworks Cybersecurity Package

Release Notes

(September 12, 2017)

docs.cloudera.com

Hortonworks Cybersecurity Package: Release Notes

Copyright © 2012-2017 Hortonworks, Inc. Some rights reserved.

Hortonworks Cybersecurity Package (HCP) is a modern data application based on Apache Metron, powered by Apache Hadoop, Apache Storm, and related technologies.

HCP provides a framework and tools to enable greater efficiency in Security Operation Centers (SOCs) along with better and faster threat detection in real-time at massive scale. It provides ingestion, parsing and normalization of fully enriched, contextualized data, threat intelligence feeds, triage and machine learning based detection. It also provides end user near real-time dashboards.

Based on a strong foundation in the Hortonworks Data Platform (HDP) and Hortonworks DataFlow (HDF) stacks, HCP provides an integrated advanced platform for security analytics.

Please visit the Hortonworks Data Platform page for more information on Hortonworks technology. For more information on Hortonworks services, please visit either the Support or Training page. Feel free to Contact Us directly to discuss your specific needs.

Table of Contents

List of Tables

1. Hortonworks Cybersecurity Suite 1.3.0 Release Notes

This document provides the latest information about the Hortonworks Cybersecurity Package (HCP) powered by Apache Metron release 1.3.0 and its product documentation.

- Apache Component Support [1]

- New Features [1]

- Platform Support Matrices [2]

- HCP 1.3.0 Repositories [4]

- Third-Party Licenses [4]

- Known Differences Between HCP 1.3.0 and Apache Metron 0.4.1 [4]

- Documentation Errata [5]

1.1. Apache Component Support

Component Versions

HCP is built on HDP 2.6.2 and HDF 3.0.1.1 and later. The official Apache versions of all HCP 1.3.0 components are:

- Apache Metron 0.4.1

- HDP supported component versions

All components listed are official Apache releases of the most recent stable versions available.

The Hortonworks approach is to provide patches only when necessary, to ensure the interoperability of components. Unless you are explicitly directed by Hortonworks Support to take a patch update, each of the HCP components should remain at the following package version levels, to ensure a certified and supported copy of HCP 1.3.0.

Note

For information on open source software licensing and notices, please refer to the Licenses and Notices files included with the software install package.

1.2. New Features

HCP is a cybersecurity application framework that provides the ability to parse diverse security data feeds, enrich, triage, and store the data at scale, and detect cybersecurity anomalies. HCP 1.3.0 provides the following new features:

- [Alerts user interface](#)

  - Displaying alerts

  - Searching alerts

  - Saving searches

  - Viewing your recent and saved searches

  - Configuring Alerts table

- Significant performance improvement for parsing

- M-pack based installation and configuration for Profiling

- Performance improvement for Indexing

- Additional geospatial and hash functions in Stellar

- Short circuit evaluation and multi-line Stellar statements

1.3. Platform Support Matrices

This section outlines the platform support matrices for HCP 1.3.0.

- Operating System Support Matrix [2]

- JDK Support Matrix [2]

1.3.1. Operating System Support Matrix

Unless otherwise noted, the following operating systems are validated and supported for HDP 2.6.2:

Table 1.1. HDP 2.6.2 Operating System Support Matrix

Operating System	Version
CentOS (64-bit)	CentOS 6.x and CentOS 7.x
Red Hat (64-bit)	RHEL 7.0[†]
Ubuntu	Ubuntu 14.0

[†]Not validated, but supported.

1.3.2. JDK Support Matrix

Unless otherwise noted, the following Java Development Kits (JDKs) are validated and supported for HDP 2.6.2:

Table 1.2. HDP 2.6.2 JDK Support Matrix

JDK	Version
Open Source	JDK8[†‡]

JDK	Version
Oracle	JDK 8

†Not validated, but supported.

1.4. Unsupported Features

Although the following features exist within HCP 1.3.0, Hortonworks does not currently support these specific capabilities:

- Technical Preview Features [3]

- Community Features [3]

1.4.1. Technical Preview Features

The following features are available within HCP 1.3.0 but are not ready for production deployment. Hortonworks encourages you to explore these technical preview features in non-production environments and provide feedback on your experiences through the Hortonworks Community Forums.

Table 1.3. Technical Previews

Feature	Description
Stellar REPL	A REPL (Read Eval Print Loop) for the Stellar language helps in debugging, troubleshooting, and learning Stellar. Stellar transforms streaming data within Apache Storm. This REPL is intended to help facilitate creation of configurations and transformations by allowing a user to replicate data and transformations encountered in production, with rapid feedback.
Alerts user interface	A standalone user interface that connects to Elasticsearch to display alerts. You can use this UI to search alerts, save your searches, and modify the Alerts table to display Alerts in a helpful format.

1.4.2. Community Features

The following features are developed and tested by the Hortonworks community but are not officially supported by Hortonworks. These features are excluded for a variety of reasons, including insufficient reliability or incomplete test case coverage, declaration of non-production readiness by the community at large, and feature deviation from Hortonworks best practices. Do not use these features in your production environments.

Table 1.4. Community Features

Feature	Description
Vagrant-based deployment	A single-node quick deployment option intended solely for development of Metron.
Docker-based deployment	A Docker-container based deployment intended solely for development of Metron.
Ansible installs	A multi-node deployment option via Ansible.

1.5. HCP 1.3.0 Repositories

Use the following table to identify the HCP 1.3.0 repo location for your operating system and operational objectives:

Table 1.5. HCP Repo Locations

OS	Format	Download Location
RedHat Enterprise Linux / CentOS 6 (64-bit)	Repo	http://public-repo-1.hortonworks.com/HCP/centos6/1.x/updates/1.3.0.0/hcp.repo
	HCP Management Pack	http://public-repo-1.hortonworks.com/HCP/centos6/1.x/updates/1.3.0.0/tars/metron/hcp-ambari-mpack-1.3.0.0-51.tar.gz
RedHat Enterprise Linux / CentOS 7 (64-bit)	Repo	http://public-repo-1.hortonworks.com/HCP/centos7/1.x/updates/1.3.0.0/hcp.repo
	HCP Management Pack	http://public-repo-1.hortonworks.com/HCP/centos7/1.x/updates/1.3.0.0/tars/metron/hcp-ambari-mpack-1.3.0.0-51.tar.gz
Ubuntu 14.04	Repo	http://public-repo-1.hortonworks.com/HCP/ubuntu14/1.x/updates/1.3.0.0/hcp.list
	HCP Management Pack	http://public-repo-1.hortonworks.com/HCP/ubuntu14/1.x/updates/1.3.0.0/tars/metron/hcp-ambari-mpack-1.3.0.0-51.tar.gz

1.6. Upgrading to HCP 1.3.0

Upgrade instructions to HCP 1.3.0 are not currently documented. For informationon about upgrading HCP, contact Hortonworks Professional Services..

For a list of configuration changes that are non-backwards compatible, see Apache Metron Upgrading.

1.7. Third-Party Licenses

Global: Apache 2.0

Apache Component	Subcomponents	License
Storm	Logback	EPL

1.8. Known Issues

The HCP 1.3.0 release has the following known issues:

Alerts UI   ACTIONS menu - The status buttons are non-functional.

Alert Status   The alert-status column displays **New** as the status for all alerts, even if the alert status is not New.

1.8.1. Known Differences Between HCP 1.3.0 and Apache Metron 0.4.1

The following Apache bugs identify known differences between HCP 1.3.0 and Apache Metron 0.4.1.

https://issues.apache.org/jira/browse/METRON-1146

Table 1.6. Known Differences Between HCP 1.3.0 and Apache Metron 0.4.1

Feature	Description
METRON-938	"service metron-rest start <password>" does not work on CentOS 7.
METRON-1156	Simulate Triage Rules in the Stellar REPL
METRON-1161	Add ability to edit parser command line options in the management UI
METRON-1185	Stellar REPL does not work on a kerberized cluster when calling functions interacting with HBase
METRON-1146	Add ability to parse JSON string into JSONObject for Stellar

1.9. Documentation Errata

There are no late additions or corrections to the product documentation for this release.